Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-14. (cancelled)

15. (New) A network device comprising:

an interface to receive a plurality of packets from a network;

a first memory to store the packets;

a controller to coordinate transfer of the packets to and from the memory;

a packet processor to perform a plurality of processing operations on the packets that are retrieved from the memory, wherein the packet processor includes a second memory to store a first portion of a control policy; and

a third memory to store a second portion of the control policy, wherein the packet processor is configured to:

apply the first portion of the control policy to at least one of the retrieved packets,

search the third memory for the second portion of the control policy, and

apply, following the search, the second portion of the control policy to the at least one retrieved packet.

16. (New) The network device of claim 15, wherein the first portion of the control policy includes a pointer to the second portion of the control policy.

17. (New) The network device of claim 15, wherein the packet processor further includes at least two of a direct memory access engine, a firewall engine, an encryption/decryption engine, or an authentication engine.

18. (New) The network device of claim 17, wherein the at least two engines are configured to operate in parallel with respect to the second packet.

19. (New) The network device of claim 18, wherein the parallel operations do not degrade a performance of either of the at least two engines.

20. (New) The network device of claim 15, wherein the plurality of processing operations include at least two of authentication, encryption, decryption, virtual private network (VPN), or firewall services.

21. (New) The network device of claim 20, wherein the at least two operations are performed in parallel with respect to the second packet.

22. (New) The network device of claim 15, wherein the plurality of processing operations include at least two of data encryption standard (DES) encryption, message

digest 5 (MD5) authentication, triple DES encryption, or secure hash algorithm (SHA1) authentication.

23. (New) The network device of claim 22, wherein the at least two processing operations are performed in parallel with respect to the second packet without causing interruption to either of the at least two processing operations.

24. (New) The network device of claim 22, wherein the packet processor is further configured to initiate a first of the at least two processing operations within a plurality of clock cycles following an initiation and without interruption of a second of the at least two packet processing operations.

25. (New) A method comprising:

receiving, at a network device, a plurality of packets from a first network which are destined for a second network;

transferring, via a first bus, a first one of the received packets for storage within the network device;

retrieving, via a second bus, the first packet from storage; and

performing a plurality of security-related packet processing operations on the retrieved packet, and concurrently transferring, via the first bus, a second one of the received packets for storage within the network device.

26. (New) The method of claim 25, wherein the plurality of security-related packet processing operations comprise at least two of authentication, encryption, decryption, virtual private network (VPN), or firewall services.

27. (New) The method of claim 26, wherein the at least two security-related packet processing operations are performed in parallel.

28. (New) The method of claim 26, wherein a first of the at least two security-related packet processing operations is initiated within a plurality of clock cycles following an initiation and without interruption of a second of the at least two security-related packet processing operations.

29. (New) The method of claim 25, wherein the plurality of security-related packet processing operations comprise at least two of data encryption standard (DES) encryption, message digest 5 (MD5) authentication, triple DES encryption, or secure hash algorithm (SHA1) authentication.

30. (New) The method of claim 29, wherein the at least two security-related packet processing operations are performed in parallel.

31. (New) A communication system comprising:

means for receiving a plurality of packets from a network;

means for storing the packets;

means for coordinating transfer of the packets to and from storage;

means for performing a plurality of security-related processing operations on the packets that are retrieved from storage;

means for conveying a first one of the packets between the means for coordinating transfer and storage; and

means for conveying a second one of the packets between storage and the means for performing security-related processing, wherein the first and second packets are conveyed concurrently.

32. (New) The communication system of claim 31, wherein the means for performing the plurality of security-related processing operations comprises:

means for achieving direct storage access,

means for screening the packets that are retrieved from storage,

means for encrypting or decrypting the packets that are retrieved from storage, and

means for authenticating the packets that are retrieved from storage.

33. (New) The communication system of claim 32, wherein the means for encrypting or decrypting the packets and the means for authenticating the packets are configured to operate in parallel with respect to the second packet.

34. (New) The communication system of claim 32, wherein the means for encrypting or decrypting the packets comprises:

means for performing at least one of data encryption standard (DES) encryption, or triple DES encryption.